US008375202B2

(12) **United States Patent**
Moore et al.

(10) **Patent No.: US 8,375,202 B2**
(45) **Date of Patent: Feb. 12, 2013**

(54) **COMMUNICATIONS METHODS AND APPLIANCES**

(75) Inventors: **Keith E. Moore**, Sunnyvale, CA (US); **Rajesh K. Shenoy**, San Jose, CA (US)

(73) Assignee: **Hewlett-Packard Development Company, L.P.**, Houston, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2886 days.

(21) Appl. No.: **10/957,490**

(22) Filed: **Sep. 30, 2004**

(65) **Prior Publication Data**

US 2006/0075221 A1 Apr. 6, 2006

(51) **Int. Cl.**

H04L 9/32	(2006.01)
H04L 9/00	(2006.01)
G09C 3/08	(2006.01)
G06F 7/04	(2006.01)
H04L 29/06	(2006.01)
G06F 21/00	(2006.01)

(52) **U.S. Cl.** **713/156**; 713/176; 726/10; 380/51

(58) **Field of Classification Search** 713/156
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,314,521 B1 * 11/2001 Debry 726/10

FOREIGN PATENT DOCUMENTS

WO WO 03093942 A2 * 11/2003

OTHER PUBLICATIONS

Mukkamala, R.; Balusani, S.;"Active certificates: a new paradigm in digital certificate management"; Parallel Processing Workshops, 2002. Proceedings. International Conference on Digital Object Identifier: 10.1109/ICPPW.2002.1039709 Publication Year: Feb. 2002 , pp. 30-37.*

"UpnPTM Security Ceremonies Design Document; "UpnP TM Device Architecture 1.0 1; Oct. 3, 2003; pp. 1-18.

"The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks;" Stajano et al.; 1999; pp. 1-11.

"HP Jet Direct Administrator's Guide;" Hewlett-Packard Development Company; 2002-2003; pp. 1-302.

"SSH IP SEC Express White Paper version 2.1"; SSH Communications Security; www.adimpleo.com/library/ssh/ipsec-wp.pdf; Aug. 1999; 31 pp.

"SEcure Neighbor Discsovery (SEND) draft-ietf-send-ndopt-06;" Arkko et al.; http://www.ietf.org/internet-drafts/draft-ietf-send-ndopt-06.txt; Jul. 17, 2004; 56 pp.

"Cryptographically Generated Addresses;" T. Aura; http://www.ietf.org/internet-drafts/draft-ietf-send-cga-06.txt; Apr. 16, 2004; 20 pp.

"IPSec Authentication Header;" S. Kent; http://www.ietf.org/internet-drafts/draft-ietf-ipsec-rfc2402bis-07.txt; Mar. 2004; 30 pp.

"IPSec Encapsulating Security Payload (ESP);" S. Kent; http://www.ietf.org/internet-drafts/draft-ietf-ipsec-esp-v3-08.txt; Mar. 2004; 39 pp.

"DHCP Secured IP Address Assignment"; http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdsiaa.htm#73568; Sep. 29, 2004; 14 pp.

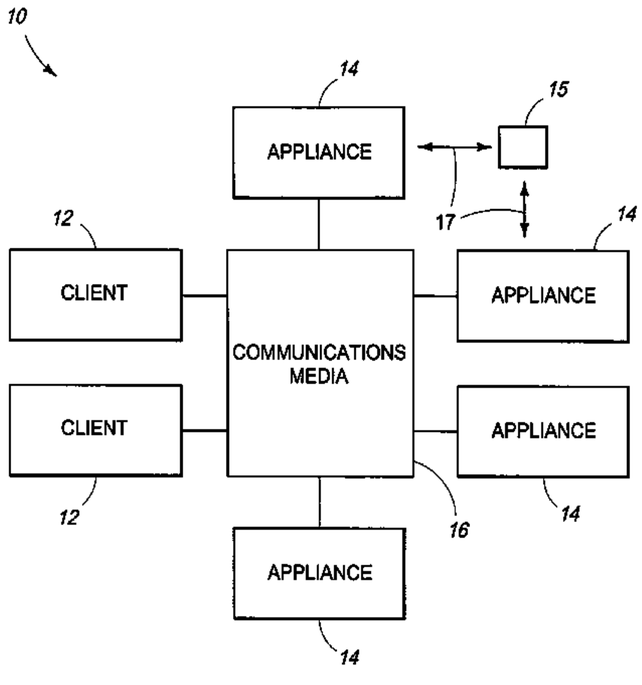
(Continued)

Primary Examiner — Andrew Nalven
Assistant Examiner — Courtney Fields

(57) **ABSTRACT**

Communications methods and appliances are described. According to one embodiment, a communications method includes prior to deployment of an appliance, establishing a trusted association between the appliance and a certificate authority, during deployment of the appliance, associating the appliance with a communications address of a communications medium, using the certificate authority, creating a signed certificate including the communications address of the appliance, announcing the signed certificate using the appliance, after the announcing, extracting the communications address of the appliance from the signed certificate, and after the extracting, verifying the communications address of the appliance.

36 Claims, 3 Drawing Sheets



OTHER PUBLICATIONS

"docs.sun.com—Sun ProductDocumentation;" Sun Microsystems; http://docs.sun.com/db/doc/816-7264/6md9iem1p?a= view; Sep. 29, 2004; 17 pp.

"Introduction to SSL;"http://developer.netscape.com/docs/manuals/security/sslin/contents.html; Oct. 1998; 10 pp.

"Security in HP Web Jetadmin;" http://h10010.www1.hp.com/wwpc/pscmisc/vac/us/product_pdfs/websecur.pdf; Nov. 2003; 8 pp.

"Electronic Device Communication Methods, Appliance Verification Methods, Appliance Programming Methods, Appliances, Articles of Manufacture, and Client Electronic Devices;" Rajesh K. Shenoy; filed concurrently.

"Configuring Security Parameters in Small Devices;" draft-hanna-zeroconf-seccfg-00.txt; Stephen Hanna; Jan. 2002; 10 pp.

"Applied Cryptography;" B. Schneirer; John Wiley and Sons; 1996. (TEXTBOOK).

"Network Security with Open SSL;" Viega et al.; O' Reily; Jun. 2002. (TEXTBOOK).

"Physical Registration: Configuring Electronic Directories using Handheld Devices;" Barton et al.; Directorieshttp://lib.hpl.hp.com/techpubs/2001/HPL-2001-119.pdf; 2001; 14 pp.

* cited by examiner

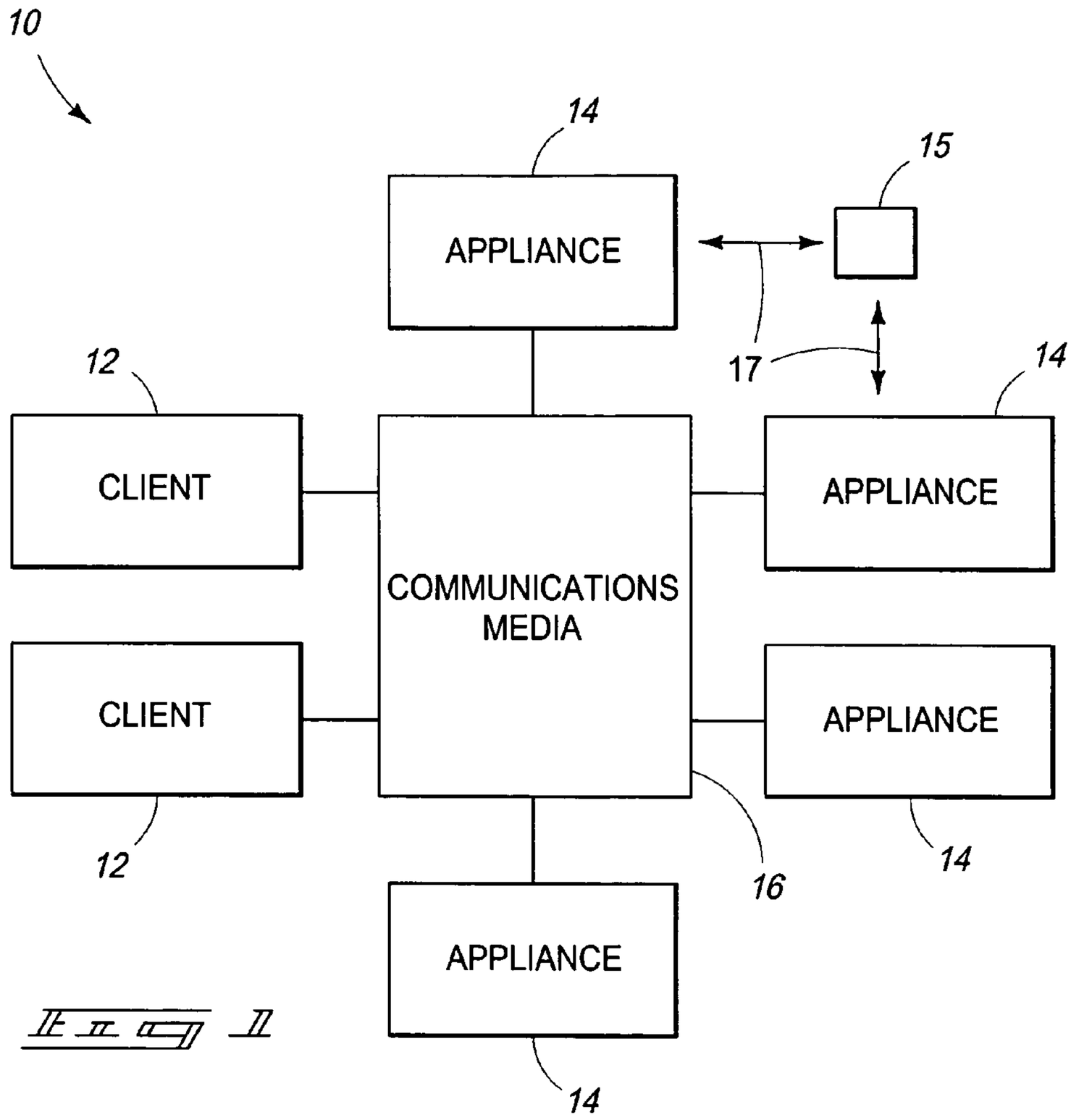

10
14
APPLIANCE
15
17
12
CLIENT
COMMUNICATIONS MEDIA
14
APPLIANCE
CLIENT
APPLIANCE
12
16
14
APPLIANCE
14

Fig. 1

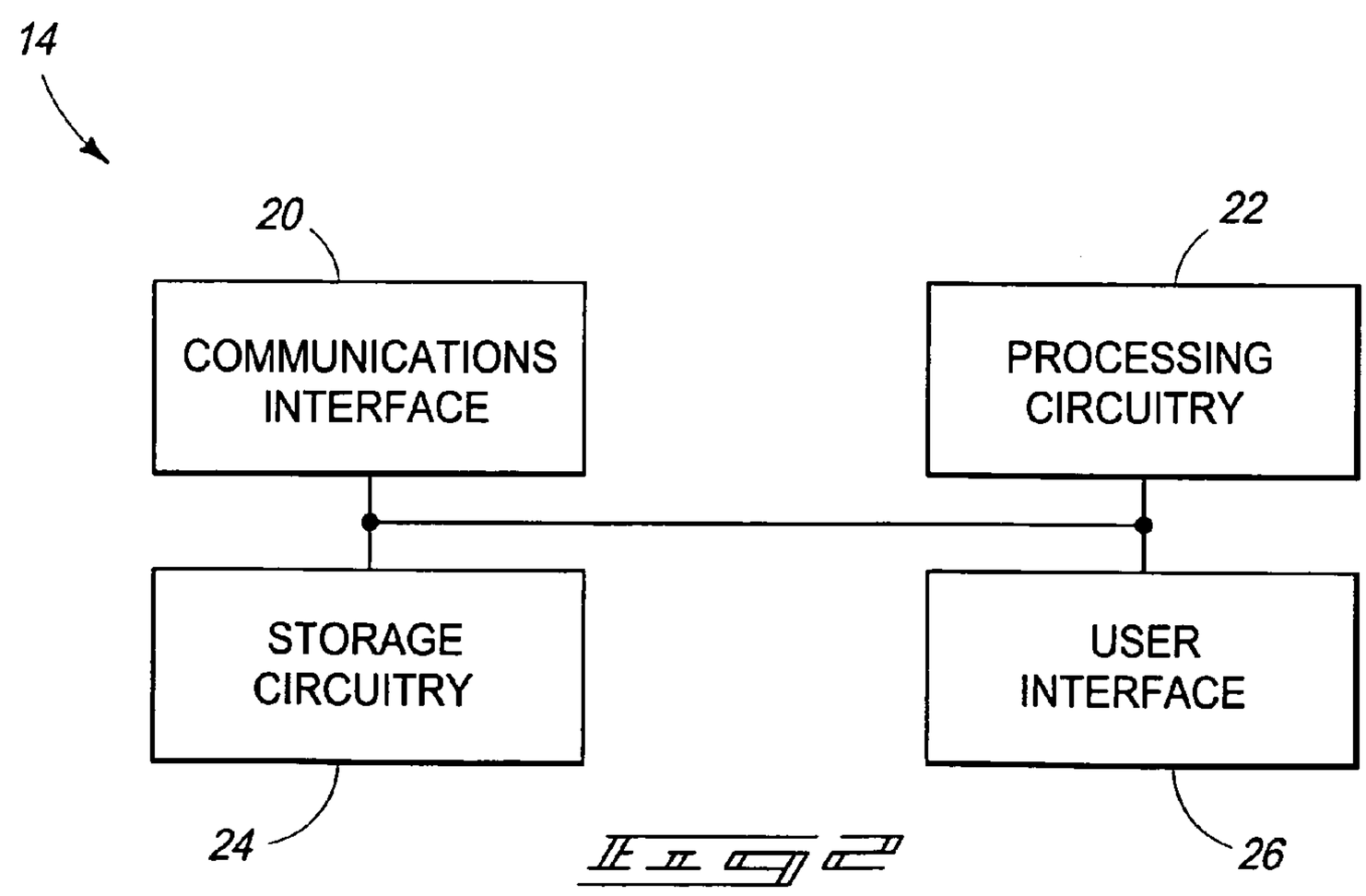

14
20
COMMUNICATIONS INTERFACE
22
PROCESSING CIRCUITRY
STORAGE CIRCUITRY
USER INTERFACE
24
26

Fig. 2

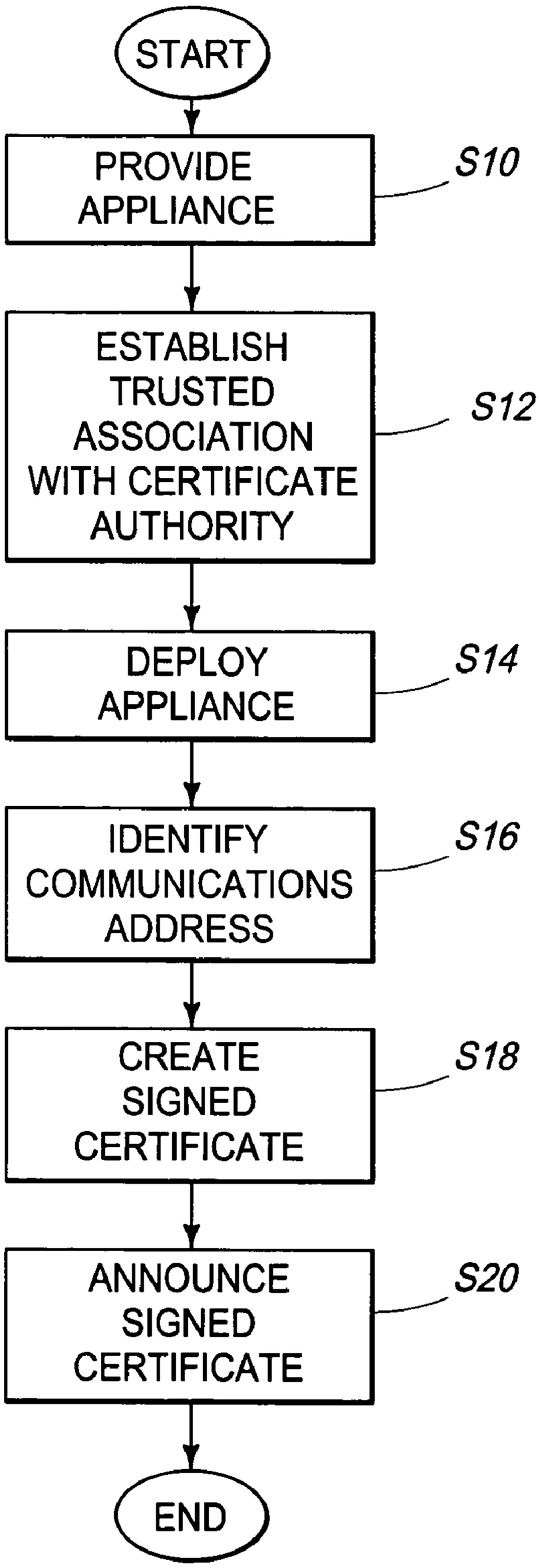

START
PROVIDE APPLIANCE
S10
ESTABLISH TRUSTED ASSOCIATION WITH CERTIFICATE AUTHORITY
S12
DEPLOY APPLIANCE
S14
IDENTIFY COMMUNICATIONS ADDRESS
S16
CREATE SIGNED CERTIFICATE
S18
ANNOUNCE SIGNED CERTIFICATE
S20
END

Fig 3

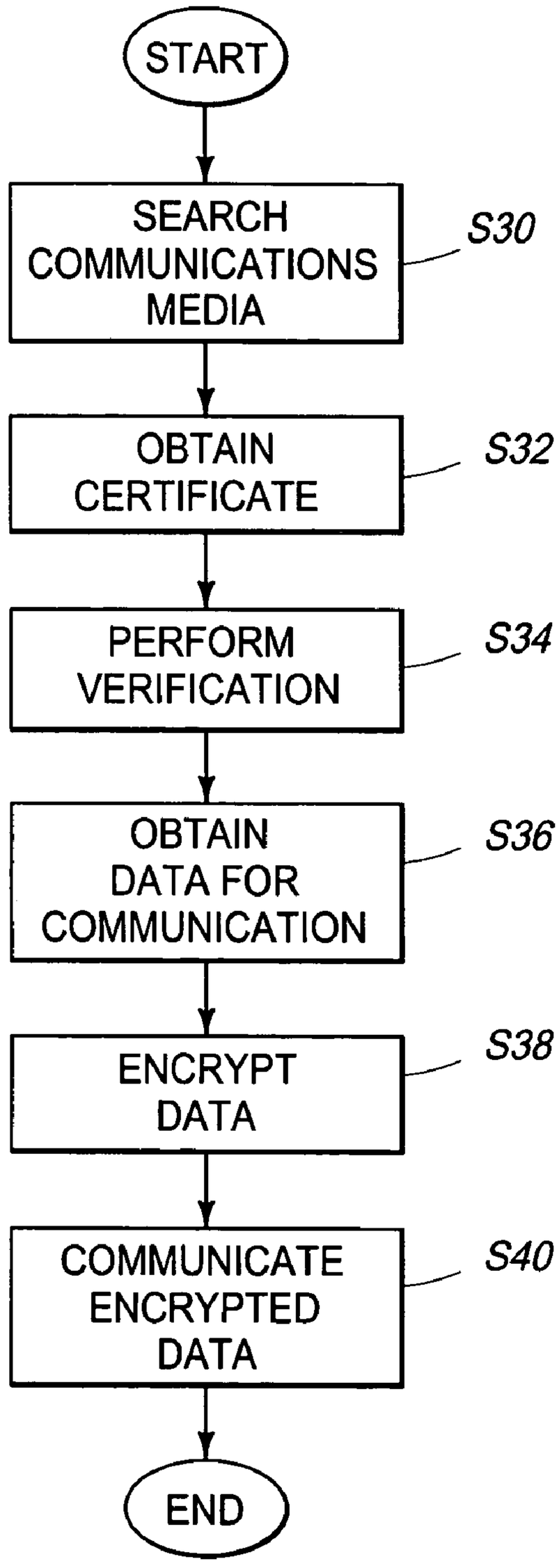

START
SEARCH COMMUNICATIONS MEDIA
S30
OBTAIN CERTIFICATE
S32
PERFORM VERIFICATION
S34
OBTAIN DATA FOR COMMUNICATION
S36
ENCRYPT DATA
S38
COMMUNICATE ENCRYPTED DATA
S40
END

Fig. 4

COMMUNICATIONS METHODS AND APPLIANCES

FIELD OF THE DISCLOSURE

Aspects of the disclosure relate to communications methods and appliances.

BACKGROUND OF THE DISCLOSURE

Over the past several years, there has been an increasing concern about the security of appliances such as disk drives, spoolers, printers, scanners and multi-functional peripherals. The concern is both around the privacy of the data being sent as well concern about whether one is interacting with the intended device or an imposter (i.e., is the printer address the one for the intended printer or a fraudulent address).

In the past, interception and "man in the middle" attacks were prevented by using 1-1 cables (such as centronix or universal serial bus). However, as appliances moved from being client peripherals to networked resources, the problem emerged of identifying the intended appliance and securing the communication to that appliance.

In the case of printers, a common approach (seen in many offices) has been to post a label of the printer name with its network address. In this manner, if an individual trusts the label, they could use that address to send a print job to the intended printer. Similar techniques are used for scanners, disk-drives, spoolers and other such appliances.

There are several problems with the label-based approach. The first is that many deployments use the dynamic host control protocol (DHCP) and thus the address of the appliance can change over time. This means that while a client might have once had the correct address, the appliance address may change and the client can easily have a misdirected message. Similarly, an imposter might intentionally mislabel an appliance such as a printer to intercept print jobs in public venues such as coffee shops or airport lounges.

Some manufacturers provide a user interface on their appliance that will report the address of the appliance on a screen or (in the case of some printers) on a printout. This helps overcome the intentional/accidental mislabeling of a device, but does not address dynamic protocol update or re-configuration of the client devices.

In addition, the above techniques do not address privacy of the transmitted data and thus eaves-droppers can intercept sensitive documents/material.

Sensitive documents can be addressed through techniques such as the secure sockets layer (SSL). In this protocol, the client and server agree on a session key that is used to encode messages exchanged between the client and server.

Other methods include IP Security Protocol (IP-Sec) which replaces the Internet Protocol with a secured packet routing mechanism. IPSec ensures that a message will be delivered only to the destination address but doesn't secure the association of the target with the address (i.e., the mechanism of discovering the correct IP address for the appliance is not addressed by either IP-Sec or SSL).

An approach to certifying the destination has been to use a challenge in the initial message from the client to the target. The challenge is encrypted with a shared secret or other keying mechanism and only the rightful recipient should be able to answer the challenge and thereby affirm the identity. The issue here is one of key distribution. If the key is shared across a family of appliances, then the imposter can redirect the print job to a second printer and intercept the material. If the key is particular to a printer, then discovering that key is an issue and similar to discovering the printer's IP address noted above.

Thus there remains a need to discover the provenance of an appliance's address, and/or to communicate with that appliance in a secure manner. At least some aspects of this disclosure are related to improved apparatus and methods for implementing electronic communications between electronic devices such as an appliance and a client in one embodiment.

SUMMARY

According to some aspects, communications methods and appliances are described.

According to one embodiment, a communications method comprises prior to deployment of an appliance, establishing a trusted association between the appliance and a certificate authority, during deployment of the appliance, associating the appliance with a communications address of a communications medium, using the certificate authority, creating a signed certificate including the communications address of the appliance, announcing the signed certificate using the appliance, after the announcing, extracting the communications address of the appliance from the signed certificate, and verifying the communications address of the appliance.

According to another embodiment, an appliance comprises a communications interface configured to implement communications of the appliance with respect to a client via a communications medium after deployment of the appliance with respect to the communications medium, wherein the appliance is associated with a communications address of the communications medium upon deployment of the appliance and wherein a trusted association is established between a certificate authority and the appliance prior to deployment of the appliance, and processing circuitry coupled with the communications interface and wherein the processing circuitry is configured to access the communications address, to initiate creation of a signed certificate using the certificate authority and which includes the communications address, and to initiate announcement of the signed certificate including the communications address for use in verification of the communications address of the appliance.

DESCRIPTION OF THE DRAWINGS

FIG. **1** is a functional block diagram of a communications system according to one embodiment.

FIG. **2** is a functional block diagram of an electronic device appliance according to one embodiment.

FIG. **3** is a flow chart illustrating an exemplary method for providing a signed certificate according to one embodiment.

FIG. **4** is a flow chart illustrating an exemplary method for implementing communications according to one embodiment.

DETAILED DESCRIPTION

Referring to FIG. **1**, an exemplary configuration of a communications system **10** is shown. Additional embodiments and aspects are described in a co-pending application entitled "Electronic Device Communication Methods, Appliance Verification Methods, Appliance Programming Methods, Appliances, Articles Of Manufacture, And Client Electronic Devices," listing Rajesh Krishna Shenoy as inventor, filed the same day as the present application, U.S. patent application Ser. No. 10/957,312, the teachings of which are incorporated herein by reference.

Communications system **10** may include one or more electronic device clients (i.e., clients) **12**, one or more electronic device appliances (i.e., appliances) **14**, one or more external communications device **15**, and communications media **16**. In one example, communications system **10** is embodied as a networked arrangement of clients **12** configured to use the resources of appliances **14**. Exemplary clients **12** include personal computers, workstations, and other electronic devices configured to implement electronic communications with respect to appliances **14** or other devices. Exemplary appliances **14** may have resources which may be accessed and used by clients **12** and may be embodied as printers, multifunctional peripherals, facsimile machines, scanners, copiers, disk drives, spoolers or other configurations accessible by clients **12**. In one embodiment, appliances **14** may comprise user-accessible devices which are configured to interact with a user during normal operation such as providing data to a user (e.g., provide printed media, copying media, displaying data, capturing data such as images, etc.). Exemplary users may include lay (i.e., non-technical) people as opposed to IT personnel.

Communications media **16** includes one or more communications medium configured to communicate data intermediate clients **12** and appliances **14** of communications system **10**. For example, one or more communications medium may comprise a communications network which may be embodied as a private and/or public network and may utilize packet-switched TCP/IP communications in one implementation. In more specific examples, communications networks include a zero-configuration network, UPnP based network or an IT-administrated network. A network may include a plurality of nodes such as switches, routers or other devices (i.e., devices not typically accessed by the exemplary above-defined users during normal operations) capable of receiving electronic communications and forwarding the electronic communications to appropriate recipients.

Individual ones of clients **12** and appliances **14** and other electronic devices configured to communicate using communications media **16** may be individually considered to be associated with communications media **16** and may have a respective unique communications address identifying the association and usable by communications media **16** and communicating devices to direct communications to appropriate recipients as well as identify a respective sending device of communications.

As described further below, clients **12** and/or appliances **14** may be configured to communicate verification information and data content using a single communications medium of the media **16**. Exemplary verification information includes a signed certificate usable to verify one or more aspect of a given client **12** and/or appliance **14**. Exemplary communicated data content may include data perceptible by a user during typical usage and may include email, a print job, a photograph, an electronic file, or other formatted data content convenient for communication between a sending device and a recipient device. In another embodiment, an individual communications medium may be dedicated to implement communications of verification information while another individual different communications medium may be dedicated to implement communications of data content. Other embodiments are possible.

Further, according to additional aspects another communications medium **17** may be configured to initiate verification operations of a client **12** and/or an appliance **14** as described further below. For example, communications device **15** is configured to utilize a communications medium **17** (e.g., electromagnetic energy) to implement communications external of communications media **16** in one embodiment. Communications device **15** and one or more client **12** and/or appliance **14** may be configured to communicate with one another apart from communications media **16**. Communications medium **17** includes any appropriate configuration and may provide wired and/or wireless communications. In yet another aspect, verification operations may be initiated using communications of media **16**.

Referring to FIG. **2**, an exemplary configuration of an appliance **14** is shown. The depicted appliance **14** includes a communications interface **20**, processing circuitry **22**, storage circuitry **24** and a user interface **26**. Other circuitry or components may be provided in other embodiments and corresponding to the respective implementation or configuration of appliance **14** (e.g., appliance **14** may include a print engine in a printer configuration). In addition, individual clients **12** may be similarly configured as appliance **14** in one arrangement and may individually include a communications interface, processing circuitry, storage circuitry and a user interface as well as any additional components or circuitry applicable to the respective implementation of client **12**.

In one embodiment, processing circuitry **22** may comprise circuitry configured to implement desired programming. For example, processing circuitry **22** may be implemented as a processor and/or other structure configured to execute executable instructions including, for example, software and/or firmware instructions. Other exemplary embodiments of processing circuitry include hardware logic, PGA, FPGA, ASIC, state machines, and/or other structures. These examples of processing circuitry **22** are for illustration and other configurations are possible. Processing circuitry **22** may formulate communications for external communication, process received communications; implement exemplary secure communications procedures described herein, and/or control and/or monitor other operations of the respective device in one embodiment. In some arrangements, a certificate authority may be embodied or embedded within appliance **14** and processing circuitry **22** may perform certificate authority operations with respect to signing certificates or other operations.

Storage circuitry **24** is configured to store electronic data and/or programming such as executable instructions (e.g., software and/or firmware), data, or other digital information and may include processor-usable media. Processor-usable media includes any article of manufacture which can contain, store, or maintain programming, data and/or digital information for use by or in connection with an instruction execution system including processing circuitry in the exemplary embodiment. For example, exemplary processor-usable media may include any one of physical media such as electronic, magnetic, optical, electromagnetic, infrared or semiconductor media. Some more specific examples of processor-usable media include, but are not limited to, a portable magnetic computer diskette, such as a floppy diskette, zip disk, hard drive, random access memory, read only memory, flash memory, cache memory, and/or other configurations capable of storing programming, data, or other digital information. As described further below, storage circuitry **24** may be configured to store certificates, keys (e.g., public and private) and other desired information.

User interface **26** may include a display configured to depict information to a user as well as a keyboard or other input device configured to receive input from a user.

At least some aspects described herein are directed towards implementing communications of increased security intermediate plural devices such as clients **12** and appliances **14**. For example, as described below, exemplary aspects provide

verification operations which enable an appropriate client **12** to certify the provenance or authenticity of a communications address of a respective appliance **14**.

According to one embodiment, an individual appliance **14** may be associated with a certificate authority (CA). In accordance with the described embodiment, a trusted association is established between the appliance **14** and the certificate authority to provide verification operations, such as certification of the provenance of the communications address of the appliance **14**, at a later moment in time. The trusted association may be established via a unique secret (e.g., prime number) shared between the appliance **14** and the certificate authority in one arrangement. In another arrangement, the certificate authority may be physically associated with appliance **14** (e.g., embodied or embedded internally of appliance **14** as mentioned above) to establish the trusted relationship, or the trusted relationship may be provided in any other appropriate manner. A source (e.g., manufacturer) of appliances **14** may have a trusted relationship with a certificate authority and through the relationship the source is able to produce serial numbers of individual appliances **14** which illustrate that the respective appliances **14** were trusted by the source and the source was trusted by the certificate authority (i.e., appliances **14** were authentically manufactured by the source also referred to as non-repudiation).

After manufacture, an appliance **14** may be deployed for operation. For example, during deployment, an appliance **14** may be associated with communications medium **16** to interact with clients **12** and perhaps other appliances **14**. During the association, a communications address of the communications medium **16** may be assigned to the respective appliance **14**. Thereafter, communications may be implemented between the appliance **14** and communications medium **16** using the communications address. Exemplary aspects are described below enabling the certification of the provenance of the communications address of the appliance **14** to provide communications intermediate clients **12** and the appliance **14**. According to some aspects, a plurality of communications addresses may be associated with an individual appliance **14**. For example, the addresses may be respectively used at appropriate moments in time (e.g., communications occur inside or outside of a firewall, etc.). The plurality of communications addresses may be provided within a signed certificate for announcement by appliance **14** described further below.

The certificate authority may create a signed certificate which includes the communications address(es) associated with the appliance **14**. After creation, the signed certificate may be stored internally of the respective appliance **14** in one embodiment.

Appliances **14** individually make their respective communications addresses available to clients **12** and perhaps other devices of the communications system **10** using respective signed certificates according to some aspects. Appliances **14** may announce respective signed certificates responsive to detection of an action such as one or more triggering event. In one example, external communications device **15** may be configured to initiate verification operations performed by one or more appliance **14** to provide the triggering event. In a more specific exemplary embodiment, device **15** may emit an external communication (e.g., according to a Bluetooth protocol) which when received by an appliance **14** initiates the receiving appliance **14** to output the signed certificate which may be utilized to certify the provenance of the communications address of the appliance **14** as described in further detail below. For example, client **12**, appliance **14** and/or communications device **15** may provide proximity reader communications to initiate the communications of the signed certificate.

In yet another possible embodiment, communications from external communications device **15** to initiate verification operations may be communicated using communications media **16**. In another embodiment, a user may access a user input of user interface **26** at an appropriate moment in time to initiate the outputting of the signed certificate from the appliance **14**. In another implementation, processing circuitry **22** of appliance **14** may monitor time intervals and initiate the communication of the signed certificate following the detection of an action including an elapse of a predetermined period of time (e.g., to provide periodic communications of the signed certificate). Other triggering events may be used in other aspects.

As described above according to exemplary embodiments, appliances **14** announce the signed certificates including outputting internally stored signed certificates. In some embodiments, announcement of the signed certificates may be independently initiated by appliances **14** or responsive to external stimulus. In additional embodiments, appliances **14** may encode or encrypt signed certificates prior to announcement of the certificates for subsequent decoding or decryption by clients **12**.

In one communications example mentioned above, communications media **16** may comprise a first communications medium for communications of data content and a second communications medium for communications of the signed certificates. A medium comprising a networking protocol may be used for communicating the signed certificates wherein the certificates can individually be sent to multiple participants (e.g., clients **12**) during a single announcement. Clients **12** may listen on the medium comprising a multicast channel for the signed certificates according to the presently described example and thereafter utilize the first communications medium to provide communications of data content if the provenance of the communications address of the respective appliance **14** is certified.

Clients **12** may access the announced signed certificates to certify the provenance of the communications addresses of the appliances **14**. In some arrangements, clients **12** are individually configured to search for the presence of the announced signed certificates. The announcements may individually include an appropriate identifier which indicates to clients **12** that a signed certificate is contained therein. Other embodiments are possible to provide for the communication of the signed certificates from appliances **14** to clients **12**.

Clients **12** receiving signed certificates are arranged to verify verification information (e.g., communications address of appliance(s) **14**) contained therein. In a first aspect, clients **12** verify the signed certificates themselves and thereafter verify the communications address(es) contained within the signed certificate(s). In one embodiment, clients **12** identify the signing entities of the source certificates (e.g., the respective certificate authorities). The respective appliances **14** may be verified as authentic if the signing entities of the signed certificates are proper (e.g., proper certificate authorities). Provenances of the communications addresses from selected ones of the appliances **14** may be rejected if the respective signing entities of the certificates are not proper.

Also according to the described embodiment, clients **12** extract communications addresses from the signed certificates. The clients **12** may also access information regarding respective sender addresses regarding the entities which announced the signed certificates (i.e., appliances **14**). In one verification embodiment, clients **12** are configured to com-

pare the communications addresses extracted from the signed certificates with respective ones of the sender addresses in order to certify the provenances of the respective communications addresses. If verification is proper, clients **12** may implement communications with respect to verified ones of the appliances **14**. If verification is not proper (e.g., certificates or signing entities not proper, or addresses do not match), clients **12** may disable any communications with respect to the appliances **14** and may also inform a network administrator or other appropriate personnel.

Once verification is completed, encrypted communications between clients **12** and verified appliances **14** may occur using the communications address extracted from the signed certificate. In one embodiment, a client **12** may create a session key and encode (e.g., encrypt) data content to be communicated (e.g., print job) using the session key. In one example, a client **12** may encrypt the session key with an appliance public key received in a signed certificate, attach the encrypted session key to the beginning of an encrypted message including data content, and communicate the encrypted message to appliance **14**. Accordingly, in one embodiment, clients **12** and appliances **14** may secure communications using a key derived from information contained within the signed certificate.

Additional information may also be communicated from appliances **14** to clients **12** using the signed certificates. In one exemplary embodiment, the additional information may include a manufacturing attribute of an appliance **14** which may include manufacturer and appliance identification information (e.g., manufacturer identification, model number and/or serial number) of the respective appliance **14**. Additional exemplary information which may be included in signed certificates includes physical location information of the appliance **14** (e.g., GPS coordinates, floor or mail stop location information, etc.).

Referring to FIGS. **3-4**, methods for providing certification of a provenance of a communications address of an appliance are shown according to exemplary embodiments. Other methods including more, less or alternative steps are possible.

FIG. **3** illustrates a method for generating verification information according to one embodiment.

Initially, at a step S**10**, an appliance to be deployed may be manufactured or otherwise provided.

At a step S**12**, a trusted association is established between the appliance and a certificate authority.

At a step S**14**, the appliance may be deployed including associating the appliance with communications media.

At a step S**16**, a communications address of the communications media associated with the appliance may be identified upon the deployment.

At a step S**18**, a signed certificate including the communications address of the appliance is created by the certificate authority.

At a step S**20**, the appliance announces the signed certificate including the communications address. The announcement may be implemented responsive to one or more different triggering event in exemplary embodiments and as described above.

Referring to FIG. **4**, an exemplary method is shown for using a signed certificate to implement communications in accordance with one embodiment.

At a step S**30**, a client may search an associated communications media for desired services (e.g., provided by one or more of appliances **14**).

At a step S**32**, the client may obtain one or more signed certificate responsive to the searching of step S**30**.

At a step S**34**, the client may use the signed certificate to verify the provenance of communications address(es) associated with the appliance. As described above, an exemplary verification operation includes comparing a communications address extracted from the signed certificate with a sender address from which communication of the signed certificate originated. If verification fails, the method may cease at step S**34**.

At a step S**36**, if verification is proper, the client obtains data content (e.g., a print job) for communication to the appliance.

At a step S**38**, the client encrypts the data content for example using a session key in one arrangement. Also, the client may encrypt the communication itself using for example a public key of the appliance.

At a step S**40**, the client communicates the encrypted data content to the appliance along with the encrypted session key in at least one embodiment.

The protection sought is not to be limited to the disclosed embodiments, which are given by way of example only, but instead is to be limited only by the scope of the appended claims.

What is claimed is:

1. A communications method comprising:

prior to deployment of an appliance, establishing a trusted association between the appliance and a certificate authority;

during deployment of the appliance, associating the appliance with a communications address of a communications medium;

using the certificate authority, creating a signed certificate including the communications address of the appliance;

announcing the signed certificate using the appliance;

after the announcing, extracting the communications address of the appliance from the signed certificate; and

verifying the communications address of the appliance.

2. The method of claim **1** wherein the announcing comprises announcing the signed certificate from a sender address of the appliance, and the verifying comprises comparing the communications address with the sender address of the appliance.

3. The method of claim **1** further comprising detecting a triggering event, and wherein the announcing is responsive to the detecting.

4. The method of claim **3** wherein the detecting comprises detecting a user input to the appliance.

5. The method of claim **3** further comprising receiving an external communication within the appliance, and wherein the detecting comprises detecting the receiving of the external communication.

6. The method of claim **5** wherein the associating comprises associating the appliance with the communications address of the communications medium comprising a first communications medium, and the receiving comprises receiving via a second communications medium different than the first communications medium.

7. The method of claim **3** wherein the detecting comprises detecting an elapse of a predetermined period of time.

8. The method of claim **1** after the verifying, implementing communications between the appliance and a client using the communications address of the appliance.

9. The method of claim **8** wherein the implementing comprises securing the communications using a key derived from information contained within the signed certificate.

10. The method of claim **1** wherein the communications medium comprises a first communications medium, and the announcing the signed certificate comprises announcing

using a second communications medium different than the first communications medium.

11. The method of claim **1** wherein the announcing comprises announcing the signed certificate including information regarding a manufacturing attribute of the appliance.

12. The method of claim **11** wherein the manufacturing attribute includes manufacturer and appliance identification information.

13. The method of claim **1** wherein the announcing comprises announcing the signed certificate including information regarding a physical location of the appliance.

14. The method of claim **1** further comprising providing the appliance comprising the certificate authority embedded within the appliance.

15. The method of claim **1** further comprising encoding the signed certificate prior to the announcing.

16. The method of claim **1** wherein the creating comprises creating the signed certificate comprising a plurality of communications addresses of the appliance.

17. The method of claim **1** wherein the extracting and the verifying comprise extracting and verifying using a client coupled with the communications medium.

18. The method of claim **1** wherein the verifying comprises certifying a provenance of the communications address.

19. An appliance comprising:

a communications interface configured to implement communications of the appliance with respect to a client via a communications medium after deployment of the appliance with respect to the communications medium;

wherein the appliance is associated with a communications address of the communications medium upon the deployment of the appliance and wherein a trusted association is established between a certificate authority and the appliance prior to deployment of the appliance; and

processing circuitry coupled with the communications interface and wherein the processing circuitry is configured to access the communications address, to initiate creation of a signed certificate using the certificate authority and which includes the communications address, and to initiate announcement of the signed certificate including the communications address for use in verification of the communications address of the appliance.

20. The appliance of claim **19** wherein the appliance is associated with the communications address upon deployment of the appliance with respect to the communications medium.

21. The appliance of claim **19** wherein the processing circuitry is configured to detect a triggering event and to initiate the announcement of the signed certificate responsive to the detection.

22. The appliance of claim **21** further comprising a user interface configured to receive the triggering event comprising a user input.

23. The appliance of claim **21** wherein the communications interface is configured to receive the triggering event comprising an external communication.

24. The appliance of claim **23** wherein the communications medium comprises a first communications medium, and the external communication is received via a second communications medium different than the first communications medium.

25. The appliance of claim **21** wherein the processing circuitry is configured to detect the triggering event comprising an elapse of a predetermined period of time.

26. The appliance of claim **19** wherein the communications medium comprises a first communications medium, and wherein the processing circuitry is configured to initiate the announcement via a second communications medium different than the first communications medium.

27. The appliance of claim **19** wherein the signed certificate comprises information for use in implementing encoded communications between the client and the appliance.

28. The appliance of claim **19** wherein the signed certificate comprises information regarding a manufacturing attribute of the appliance.

29. The appliance of claim **28** wherein the manufacturing attribute includes manufacturer and appliance identification information.

30. The appliance of claim **19** wherein the signed certificate comprises information regarding a physical location of the appliance.

31. The appliance of claim **19** wherein the certificate authority is embedded within the appliance.

32. The appliance of claim **19** wherein the processing circuitry is configured to encode the signed certificate before the initiation of the announcement.

33. The appliance of claim **19** wherein the signed certificate comprises a plurality of communications addresses of the appliance.

34. The method of claim **1** wherein the announcing the signed certificate comprises outputting the signed certificate externally of the appliance.

35. The method of claim **1** wherein the verifying comprises verifying using the communications address extracted from the signed certificate.

36. The appliance of claim **19** wherein the processing circuitry is configured to initiate the announcement of the signed certificate in the absence of any communications received by the appliance.

* * * * *